SEGURIDAD INFORMÁTICA ¿VULNERABILIDADES TÉCNICAS O ERRORES HUMANOS?

Por: Emilio Zaidman

La disciplina de la seguridad informática se ha ido sofisticando cada vez más, y si bien es cierto que cada vez hay más herramientas, dispositivos e información sensible para resguardar y por lo tanto pasible de ser atacada, la mayor cantidad de las incidencias de seguridad se siguen debiendo, como desde hace años, a errores humanos. **Según distintos informes a nivel mundial, entre un 90 y un 95 por ciento de los ataques o incidentes en materia de seguridad, se deben finalmente a fallas humanas.**

Sin embargo, cada vez que sale a la luz un incidente de seguridad informática de alto impacto, poco foco se pone sobre los puntos débiles, o las vulnerabilidades sobre las cuáles el evento actuó, y mucho hincapié se hace sobre las cuestiones técnicas y tecnológicas de gran sofisticación.

Esto ocurrió hace muy poco tiempo con la aparición de un virus que tuvo un impacto pocas veces visto a nivel mundial. Repasemos un poco de qué se trató e intentemos aprender de lo sucedido para traducir las herramientas con las que contamos para blindarnos ante estos ataques.

¿Qué pasó?

El viernes 12 de mayo de 2017 comenzó un ciberataque mundial, denominado *WannaCry*, que apuntó a los equipos que ejecutan el sistema operativo *Microsoft Windows*, cifrando datos y exigiendo pagos de rescate en la moneda *Bitcoin* (ver recuadro: ¿Qué es *Bitcoin*?). El mismo incluyó instrucciones para enviar entre US$ 300 y US$ 600 a ciertas direcciones *Bitcoin*, las cuales están vinculados a cuentas de acceso público, por lo general llamadas billeteras.

¿QUÉ ES BITCOIN?

El *Bitcoin* es un medio digital de intercambio, que hace referencia tanto a la moneda como al protocolo y a la red P2P (*Peer to Peer* o Punto a Punto) en la que se apoya. Lo que hace distinto al *Bitcoin* frente a las monedas tradicionales y otros medios de pago virtual, es la descentralización. Es decir, está fuera del control de cualquier gobierno, institución o entidad financiera.

El control lo realizan los propios usuarios a través de los intercambios P2P. Esta estructura imposibilita, en principio, que cualquier autoridad manipule su valor.

La descentralización y el anonimato, la han convertido sin embargo en el medio de pago “oficial” de los cobros extorsivos como el *ransomware*.

Sobre el autor

EMILIO ZAIDMAN

LICENCIADO EN ADMINISTRACIÓN, 39 AÑOS, DOCENTE DE LA CÁTEDRA DE ADMINISTRACIÓN DE LOS RECURSOS DE INFORMACIÓN EN LA FCE-UNLP, CON MÁS DE 15 AÑOS DE EXPERIENCIA EN DISTINTAS POSICIONES VINCULADAS A LA TECNOLOGÍA INFORMÁTICA Y A LAS TELECOMUNICACIONES. ACTUALMENTE, SE ENCUENTRA TERMINANDO UN MÁSTER EN GESTIÓN DE TECNOLOGÍA INFORMÁTICA EN *GEORGE WASHINGTON UNIVERSITY, WASHINGTON DC, EEUU.*

EMAIL: EMILIO.ZAIDMAN@ECONO.UNLP.EDU.AR

Esta agresión se encuadra dentro de los llamados *Ransomware*, un tipo de software malicioso que ejecuta un ataque de tipo extorsivo, bloqueando el acceso a los datos hasta que se paga un rescate. Por consiguiente, se encuadra dentro de las llamadas técnicas de denegación de acceso (*DoS*, en inglés) que impide que los usuarios accedan a los archivos, ya que no es posible descifrarlos sin la clave de descifrado. Se realizan típicamente usando un troyano, que tiene un *software* malicioso disfrazado como un archivo legítimo e inofensivo. A menudo este tipo de ataques, se transmite por correo electrónico o *pop-ups* en la web.

El acontecimiento se ha descrito como sin precedentes en su escala, infectando más de 230.000 computadoras en más de 150 países. Los países más afectados han sido: Rusia, Ucrania, India y Taiwán, pero partes del Servicio Nacional de Salud de Gran Bretaña, la empresa española Telefónica, FedEx y LATAM Líneas Aéreas, también fueron impactados; junto con muchos otros países y compañías por todo el mundo.

En Argentina, si bien tuvo relativamente pocos reportes (algunas fuentes estiman menos de 5.000), muchos usuarios se vieron particularmente expuestos debido a la alta proporción en el uso de *Microsoft Windows*, y a la baja propensión a utilizar software actualizado.

La variedad de *ransomware* que se utilizó, llamada *"Wanna Decryptor"*, explotó una vulnerabilidad en *Microsoft*. Llamativamente, *Microsoft* publicó un parche el 14 de marzo de 2017, casi dos meses antes del ataque, para eliminar la vulnerabilidad subyacente a los sistemas soportados. Aún así, muchas organizaciones y usuarios individuales, no lo habían instalado.

¿Por qué el ataque tuvo este impacto a nivel mundial?

Si bien no hay una única respuesta, el ataque fue destinado en general, a una cuestión de recursos y atención. Este podría haberse evitado si muchas empresas simplemente hubieran mantenido sus máquinas al día con el último *software*. Pero, en realidad, hacer esto puede ser más difícil de lo que parece, ya sea por culturas corporativas que no dan prioridad a la seguridad o por falta de fondos para actualizar las últimas versiones de *software.*

¿Cómo protegerse?

Como se mencionó, cada vez que salen a la luz estos ataques, se hace mucho hincapié sobre el impacto y las vulnerabilidades a nivel técnico, pero poco sobre las herramientas con que contamos, la mayoría de las cuales son realmente sencillas, aunque impliquen frecuentemente cambios en las pautas de uso de los dispositivos y las redes.

Actualización del *Software.* Particularmente este ataque se hubiera evitado si los dispositivos se encontraban actualizados, especialmente aquellos que aún utilizan *Windows XP.* Las actualizaciones de *software,* a menudo contienen

muchos parches que corrigen errores y cierran vacíos de seguridad. Se pueden, por ejemplo, configurar los dispositivos para que instalen las actualizaciones automáticamente. Los *hackers*, sin embargo, se aprovechan usualmente del exceso de confianza de los usuarios en este sentido.

Copias de Seguridad. Asimismo, se deben crear copias de seguridad de los archivos más importantes, ya sea descargandolos en un disco duro externo o almacenándolos en un servicio de almacenamiento basado en la nube. Existen hoy en día decenas de servicios gratuitos o de muy bajo costo para realizar copias de seguridad en la nube. Y también, decenas de herramientas (gratuitas y comerciales) que llevan a cabo esta operación de forma automática, y que sólo requieren una configuración inicial de unos minutos.

Contraseñas de seguridad. Si bien mucho se ha escrito y sugerido sobre el uso y actualización de las contraseñas, quizás la sugerencia más sencilla es que se lleve a cabo un uso y seguimiento de las contraseñas en forma única para cada uno de sus servicios. Es un tanto contra intuitivo, pero es más seguro que la alternativa de reutilizar la misma contraseña en varios sitios web. De esta manera, se deberían usar contraseñas más complejas para aquellos servicios más riesgosos (servicios de banca digital, o *home banking*, redes sociales, etc.), y otras más fáciles de recordar para subscripciones online y demás servicios de bajo riesgo.

Correos sospechosos. Recuerde tratar los correos electrónicos inesperados con precaución y tener en cuenta el *"phishing"* - uno de los tipos más comunes de ataques de ingeniería social utilizados. No abrir nunca correos sospechosos, así provengan de personas conocidas. Si vienen en inglés, con redacción extraña, o sin texto en el cuerpo, pero con un adjunto, por ejemplo. Si un correo electrónico parece haber venido de su banco, empresa de tarjeta de crédito o proveedor de servicios de Internet, tenga en cuenta que nunca le pedirán información sensible como su contraseña.

Antivirus. También se recomienda, en general, instalar *software* antivirus. Si bien muchos usuarios descreen de la protección que brindan, para el caso particular antes mencionado, el 30 por ciento de los sistemas antivirus más populares eran capaces de detectar y neutralizar el *ransomware*. Por supuesto, el mismo principio se aplica: asegurarse de mantener la aplicación actualizada para que sea capaz de bloquear los últimos *malware* emergentes. Igualmente, se debe asegurar que el antivirus sea confiable.

Cree un plan de seguridad para la empresa. Para las empresas, la implementación de actualizaciones de seguridad en toda la organización puede ser difícil. Si la PC de un empleado carece del *software* de seguridad más reciente, puede infectar otras máquinas a través de la red de la empresa.

Por estos motivos, los profesionales en tecnologías de la información deben poner el foco en educar a los usuarios, y probar regularmente a los empleados para detectar correos electrónicos sospechosos y otros riesgos potenciales.

En cuanto a los profesionales en ciencias económicas, deben identificar los datos y la información más sensible en cada una de las áreas, para establecer medidas prioritarias en su protección. Esto debe ser indudablemente una tarea de la gerencia o apoyada por la misma, luego de un exhaustivo relevamiento de toda la información almacenada en la empresa.

Concientización sobre la seguridad. Cuando se trata de la seguridad de los datos, los atacantes siguen aprovechándose del punto más débil de todos: las personas. La falta de concienciación o incluso el desconocimiento de amenazas como el *phishing*, pueden hacer el trabajo muy fácil para aquellos que traten de hacerse con datos personales de manera fraudulenta. Entre las omisiones más comunes vinculados al error humano, se encuentran: el ser demasiado confiados, reutilizar la misma contraseña para distintos servicios, usar *software* no autorizados, y dar datos de más en las redes sociales.